ISSN (Online): 2348-8557

International Journal of Computer Informatics & Technological Engineering

VOLUME -1, ISSUE -1, MARCH- APRIL, 2014

PAPER ID: 2014/M-A/IJCITE/V1-E1-25

IJCITE

ENHANCING DATA SECURITY THROUGH COLOR CODING ON PRIVATE CLOUD

Dr. Ritu Soni[1], Sanjay Kumar Sharma[2]

[1]Head Dept. of Computer Applications, Guru Nanak Girls College Santpura, Yamunanagar, Haryana, India -135001

[2]Assistant Professor, Dept. of Computer Science & Engineering, Chandigarh University, Gharuan, SAS Nagar, Punjab, India

Abstract: **Cloud computing envisage the IT industry as an technology driven service oriented approach that delivers the result to the enterprises by deploying the software and the databases to huge data centers where trust of the data and services may be required to be ensured by the system. This paper is written to confront the data security challenges and proposes an model that strengthens the criticality of the data on the basis of color coding.**

Keywords: ***Cloud Computing, Authentication, Criticality.***

I. INTRODUCTION

Cloud computing represents a budge to Computing as a product or service that is purchased, to computing as a service that is delivered to consumers over the internet from large-scale data centers - or 'clouds'. This research highlights research challenges for cloud computing from an enterprise or organizational perspective, and suggests a Cost Effective Integrated Hybrid Model for Enterprise Cloud Computing.

A) *Objective*: The aim of this study is to deploy the Private Cloud environment on Public Domain, so that;

- The private users can access Private Cloud on Public domain.
- The data of the Private Cloud is secured and restricts to Cloud boundaries.

While deploying this environment, Simulator is developed for security concerns that are faced during Private Cloud implementation on Public Domain.

Cloud can be deployed as Private, Public and Hybrid Domain. The Private Cloud is accessible on Private Domain only. The Public Domain is accessible across the Web. The Hybrid domain is encapsulation of Private and Public Cloud. Some Private Cloud are deployed on Public Domain and sometimes, the part of Public domain is set as proprietary thereby, making the part of Public Cloud as Private. During the deployment of Private Cloud on Public Domain, the security implications occur at the User level and Data level. The probability of accessing the Private Cloud on Public Domain is more prone to Web attacks. It needs to ensure the privacy and safety of user data which can be obtained by the malicious attacks over the cloud. As Private Cloud works on Virtualization, this also invites vulnerability to the Cloud security where virtual machines are running on a physical server and is accessed by different users even with the administrator's privilege. Cloud environment faces more security attacks has the large amount of data of various users which are stored in the cloud environment making it vulnerable and target of many attackers. Since the accessibility of the Private Cloud which is available on Public Domain has web vulnerabilities in terms of User Authentication and Data Accessibility, the Simulator has been developed addressing the issues mentioned. The proposed model checks the Authenticity of the user by considering the fingerprints and data severity to authorized users by marking the critical data as red. The Critical Data would

ISSN (Online): 2348-8557
International Journal of Computer Informatics & Technological Engineering
VOLUME -1, ISSUE -1, MARCH- APRIL, 2014
PAPER ID: 2014/M-A/IJCITE/V1-E1-25
IJCITE

be visible to the Administrator and the Authorized users.

B) Benefits: In the deployment of Private cloud on Public domain, the security implications that were encountered has been resolved by setting the Accessibility level of the user and setting the criticality of the data.

II. LITERATUE SURVEY

Cloud services are usually provided to multiple tenants which is also one of the reasons that users lose their trust on the services. Moreover it is essential to secure the data at the cloud so that the vendor providing cloud services should themselves be incapable to read or access the stored data. Note the drop box security issue was caused by the software security update. Another issue with the cloud security is the local government laws in which the data stored in cloud is monitored. The security which is considered as a safe in one country might not be for other country. As the cloud computing is virtualized this is why it gets difficult to know that in which country the data is being stored. This on the other hand plays a crucial role in securing the data at remote locations as in case of natural calamities that data still remains safe [1].

As the data stored in the cloud environments does not have the control of the consumers and risks the data and environments with the vulnerabilities that could lead to the security issues in the cloud environments [2].

Hurwitz et. al., [3] has presented a better medium for storing the data as far as security is concerned when compared with the old way of storing the data in magnetic tapes like floppy drives, mainframe or hard disks. It provides in-depth knowledge about the concept and basics of cloud computing exploring the different benefits provided by cloud services like scalability which supports on-demand requirements from the customers in real time.

Zaharia et. al. [4] came out with LATE, a type of scheduling algorithm that can be used for handling heterogeneity inside cloud data center. The significance of the algorithm LATE is to schedule the tasks as per the longest approximate time for completion.

Effective provisioning of IT as technological improvement of Data Centers is required to ensure the data security at every level. [5]

III. BOUNDARY CONDITIONS

For developing such a Simulator, the following boundary conditions are finalized:

1. The parameters that are taken into consideration are the setting the Authorization of the user and the setting the Criticality of the Data.
2. The criticality of the data is shown only to Authorized users and is marked in Red Color.
3. The user can access the data from the valid concerned IP location of the Cloud.
4. Whole of application has two been configured with two views - Administrative View & User View.
5. Based on the assigned credentials of the user, the logged in user can view the Dashboard for which the user is authorized.
6. In the **Administrative View**, the Authorized super user with "Administrator" designation would login with mandatory check points of Left Thumb impression and Right Thumb impression and has the following rights:
   - Create users/Delete Users/Update Users
   - During the creation of the users, at least 5 thumb impression each of the finger prints will be scanned so that the authenticated user can login through any of these finger prints impressions stored in the database.
   - Authorized the users with accessibility rights.
   - Set the Data Criticality, by setting the criticality level of the Fields/Attributes.
   - Summary of User Sessions with detailed reports on Date, Time, Logged sessions and Page accessed History.
7. In the **User View**, the user has been given the accessibility to view only.

ISSN (Online): 2348-8557

International Journal of Computer Informatics & Technological Engineering

VOLUME -1, ISSUE -1, MARCH- APRIL, 2014

PAPER ID: 2014/M-A/IJCITE/V1-E1-25

IJCITE

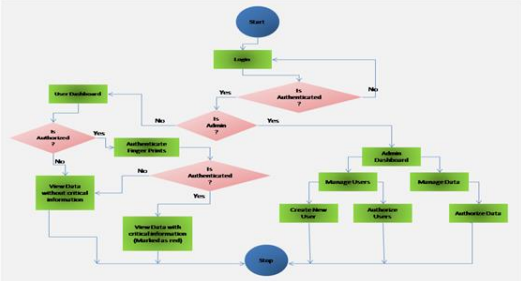

Figure 1: Diagramtic representation

IV. ALGORITHM FOR SIMULATOR

webippc()

Step 1: Read URL

call authentication_URL()

[authentication_URL() is the method to check the correctness of the valid url]

if false

call application_Exit()

[application_Exit() is the method to exit the application]

end if

Step 2: On success

call login_Page()

[login_Page() call the login page]

Step 3: Input the username and the password, on submit,

call user_Authentication()

[user_Authentication() is the method to check the authentication of the user]

Step 4: Check the User designation,

if user='Administrator'

Select choice

i) call user_Creation()

[user_Creation() is the method to create users]

ii) call user_Authorization()

[user_Authorization() is the method to set the authorization access of data]

iii) call data_Severity()

[data_Severity() is the method to set the Severity of the data]

set_colorStatus_Red()

[set_colorStatus_Red() method to show critical data]

else if user='Others'

i) call check_Roles()

[check_Roles() check the role of the user]

ii) call view_Data()

[view_Data() shows the data to the user according to the Authorization set]

Step 5: Exit

V. IMPLEMENTATION

The Simulator has been designed and implemented on Dual Core XEON Processor, having 8 GB of RAM and IIS as the Web server.

VI. VALIDATIONS INCORPORATED

Validation is the process of validating all aspects of the application from its accessibility over the web to the usage and in turn the validation of each and every entry which is available in the module. The following validations are taken into consideration.

A) URL Validation: The URL (Uniform resource locator) of the Private Cloud which is deployed on Public Domain is verified

- It should be of order https://www.myprivatecloud.com

B) User Creation: During the creation of the user, the following checkpoints have been incorporated.

- Check for existence of duplicated user.
- Check for existence of user as Alphanumeric or Character based data.
- Username to be consisting of minimum 8 characters.

C) Password Creation: During the creation of the password, the following validations has been applied.

- The password should not be of same as Username.
- The password should be of minimum 8 characters.
- The password should be of alphanumeric type and must contain at least 2 special characters and at least two alphabets in capitals.
- No two special characters must be successive.

ISSN (Online): 2348-8557
International Journal of Computer Informatics & Technological Engineering
VOLUME -1, ISSUE -1, MARCH- APRIL, 2014
PAPER ID: 2014/M-A/IJCITE/V1-E1-25
IJCITE

- The password severity is notified
- The user is notified for the change of password every month, however, it is mandate to change the password in every three months.
- Whenever, the password is changed or reset, the previous passwords are not allowed.

D) *Session Management:* When the user is logged, the session management is applied so as to have following deliverables:

- The session of the user is maintained.
- If there is no activity of the Browser, the session is automatically expired.
- Dynamic redirection of pages is check and session is maintained.
- The session checks the previous URL and also the user and maintains the tracking of swapped record.
- The session is killed on the click of Logout.

E) *Clickable Deployment:* The deployment is mandated to keep track of the following credentials:

- The clickable event gets fired if and only if the Session is active.
- Once clicked the user is directed to the respective menu.
- In case, the user saves the page as **"Bookmark" or "Favorite",** the Click event on page will not work as the session is not active and page tracking is not passed.

F) *Log Records:* The deployment maintains the log tracking of the following evnets:

- The URL accessible date and time.
- The Logged user details, time in and time out.
- The details of each Button/Link Clicked, i.e, the date, time and frequency.
- The paged accessed date and time and frequency for every session.
- The session time in and out.

G) *Cache Clearance:* It is ensured that the History and cache is cleared every time, the user is logged off from the session.

VII. DISCUSSIONS

The discussions are supported by the cases and the relevant comments.

Case 1: Login as Administrator: The URL is typed on the browser that is checked and then after its correction, the user gets the Login screen, as shown in Figure 6.1. Irrespective of the type of the user, the finger print of left and right thumb impression is scanned Figure 6.2, Figure 6.3 and Figure 6.4 respectively, and after authentication, the user is directed to Dashboard. Figure 6.5 shows the Administrator dashboard, where the Administrator can create users/Edit user details/Delete user Details, Figure 6.6 and Figure 6.7, Authorize user details Figure 6.8 and Figure 6.9. The Administrator set the severity of the data i.e. attributes as shown in Figure 6.10, and set the severity of the fields.

Case 2: Login as Others but Authorized User: When the non Administrator or Other user logins but has the Authorization to view the critical data, finger print details are asked as shown in Figure 6.11, Figure 6.12 and Figure 6.13. Since this user has the authorization to view the critical data, the fields are shown in red color whose severity were set by the Administrator as shown in Figure 6.15.

Case 3: Login as Others but Non Authorized User: When the non-Administrator or Other user logins who doesn't have the Authorization to view critical data, the attributes or the data is not even visible and hence the criticality of the data and the accessibilities are maintained as shown in Figure.

VIII. CONCLUSION

The simulator **webIppc** designed and developed applies the countermeasures on Private Cloud Deployed on Public Domain by laying the security at application as well

ISSN (Online): 2348-8557

International Journal of Computer Informatics & Technological Engineering

VOLUME -1, ISSUE -1, MARCH- APRIL, 2014

PAPER ID: 2014/M-A/IJCITE/V1-E1-25

IJCITE

as data level. The environment is set by using the Microsoft Technologies such as C# on Microsoft Visual Studio 2012, and Microsoft SQL Server 2008 R2 as the backend and configured on Internet Information Server (IIS 7.0)

The simulator **webIppc** implements the private cloud on public domain by deployment of proposed models **Data Security Color Model (DSCM)** and **Data Security Finger Print Model (DSFPM)** on web interface where the user authorization is ensured by passwords and fingerprint impressions. The authorization of the user and data severity is set by the Administrator. The authorization of the user enables the restriction of data view as per the role set. The attributes which has been marked as high severity is accessible to authorized users with the indication of the red color.

Such a simulator will be helpful for all those web environments where huge data is to be accessed by multiple users for multipurpose activities and at viewable at all locations.

Implications of web deployment do have the risk of history content, cache data, bookmarks and favorites. Along with this loading time of web page may happen to take much time in the scenarios where the page has many fields to input and has more post backs to the web server. Web exploits are quite vulnerable like URL re-writing, session hijacks, cross site scripting, SQL injections etc.

IX. REFERENCES

[01] Binning, D (2009). "Top five cloud computing security issues". Available at: http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues

[02] Carroll, M., Van der Merwe, A. and Kotze, P. (2011). "Secure cloud computing: Benefits, risks and controls". *Information Security South Africa (ISSA)*. pp: 1-9. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6027519

[03] Hurwitz, J. Bloor, R. Kaufman, M. and Halper, F. (2010). "Cloud Computing for Dummies". Available at: http://www.dummies.com/how-to/content/what-is-cloud-computing.html.

[04] Zaharia, M., Konwinski, A., Joseph, A.D. Katz, R. and Stoica, I. (2008). "Improving mapreduce performance in heterogeneous environments". *In 8th USENIX Symposium on Operating Systems Design and Implementation*. Available at: http://dl.acm.org/citation.cfm?id=1855744

[05] Soni Ritu, Sharma, Sanjay Kumar, "Design of cost effective integrated model for enterprise cloud computing", International Journal of Informative & Futuristic Research, Volume -1 Issue -4, December 2013